IN THE CLAIMS:

Please amend the claims as indicated. A complete set of the claims is included below, reflecting added subject matter *(underlining)* and deleted subject matter *(strikethrough)*, as well as the current status of each claim. This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) A method of ensuring the security of a computer system comprising a host facility and a portable computing device coupled to the host facility, comprising the steps of:

loading software suitable for operating on an open platform computer system in a secure environment on the open platform computer system comprising the host facility and the portable computing device;

upon loading the software on the open platform computer system, initiating a pre-synchronization scan;

during the pre-synchronization scan, validating the software by the use of a validator program residing in the open platform computer system in a secure fashion such that the validator program scans the software that is loaded in the secure environment;

wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures;

marking the software that is loaded as valid or invalid by the use of a flag; and,

automatically denying the software the ability to operate on any environment within the open platform computer system and denying synchronization of the software with the portable

computer device if the validator fails to identify said software as valid in order to ensure the security of the open platform computer system.

2-3. (Canceled)

4. (Previously Presented) The method described in Claim 1 wherein the software is supplied by a third-party source.

5. (Previously Presented) The method described in Claim 4 wherein the third-party software is for execution or other use on a palmtop computer.

6. (Previously Presented) The method described in Claim 1 wherein the validator program is specially constructed to reside in a secure fashion in the host facility of the open platform computer system.

7. (Previously Presented) The method described in Claim 1 wherein the method operates on a computer system which comprises:

a host computer; and

a portable computing device coupled to the host computer and wherein the validating operation is performed by the host computer for the portable computing device.

8. (Previously Presented) An apparatus for ensuring the security of an open platform computer system, comprising:

a portable computing device coupled to a host computer, wherein the portable computing device is configured to load software from the host computer to the portable computing device for operating on the portable computing device; and,

a validation program residing on the open platform computer system in a secure fashion that is configured for:

validating the software during a pre-synchronization scan by first scanning the software that is loaded in a secure environment;

wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures;

marking the software as valid or invalid by the use of a flag; and,

automatically denying the software the ability to operate in any environment on the open platform computer system and denying synchronization of the software with the portable computing device if the validator fails to identify the software as valid in order to ensure the security of the computer system.

9. (Previously Presented) The apparatus described in Claim 8 wherein the host computer is coupled to a network.

10. (Previously Presented) The apparatus described in Claim 8 wherein the portable computing device is a handheld computing device.

11. (Previously Presented) The apparatus described in Claim 8 wherein the portable computing device is a personal data assistant.

12. (Previously Presented) The apparatus described in Claim 8 wherein the portable computing device is coupled to the host computer by an infrared device.

13. (Previously Presented) The apparatus described in Claim 8 wherein the portable computing device is coupled to said host computer by an RF enabled device

14. (Previously Presented) The apparatus described in Claim 8 wherein the validation program resides in the host computer of the computer system in a fashion intended to be secure.

15. (Previously Presented) The apparatus described in Claim 8 wherein the validation program is configured to evaluate third-party software and attach a digital "valid" flag if the third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to the third-party software in the third-party software is not found to be clean of known security compromising routines.

16. (Previously Presented) The apparatus described in Claim 15 wherein the portable computing device is configured to load third-party software files with the digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have the "invalid" flag attached.

17. (Previously Presented) The apparatus described in Claim 15 wherein the portable computing device is a Personal Data Assistant.

18. (Previously Presented) An apparatus for ensuring the security of an open platform computer system, comprising:

a handheld computing device coupled to a network, wherein the handheld computing device is configured to load software from the network to the handheld computing device for operation on the handheld computing device; and,

a validation program that resides on the network that is configured for:

validating the software by scanning files of the software in a secure environment on the handheld computing device upon loading the software in any environment on the handheld computing device;

wherein the act of scanning and validating comprises running code of the software in an emulator for the open platform computer system within the secure environment for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures;

marking the software as valid or invalid by the use of a flag; and,

automatically denying the software the ability to operate on any environment on the computer system if said validator fails to identify the software as valid in order to ensure the security of the computer system.

19. (Previously Presented) The apparatus described in Claim 18 wherein the validation program resides in the network in a secure fashion.

20. (Previously Presented) The apparatus described in Claim 18, wherein the handheld computing device is configured to load third-party software files with the digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have the "invalid" flag attached.

21. (Previously Presented) The apparatus described in Claim 18 wherein the validation program is configured to evaluate third-party software and attach a digital "valid" flag if the third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to the third-party software in the third-party software is not found to be clean of known security compromising routines.

22-28. (Canceled)